CRIT LUALLEN
AUDITOR OF PUBLIC ACCOUNTS

May 1, 2008

Jon Draud, Commissioner
Department of Education
500 Mero Street
Frankfort, KY 40601

Dear Commissioner Draud,

We have audited the Department of Education as an integral part of our Single Audit of the Commonwealth of Kentucky for the year ended June 30, 2007, which includes in part the audit of the Comprehensive Annual Financial Report (CAFR). Our procedures included testing certain activities of the Department of Education for compliance and internal control over financial reporting and over requirements applicable to each major federal program. Our findings and recommendations related to those procedures are reported as described below.

Internal Control

We considered the Department of Education's internal control as a basis for designing our auditing procedures for the purpose of expressing our opinion on the Commonwealth's financial statements and for expressing opinions on the Commonwealth's compliance with requirements applicable to each major federal program, but not for the purpose of expressing an opinion on the effectiveness of internal control. Accordingly, we do not express opinions on the effectiveness of the Commonwealth's or the Department of Education's internal control.

A control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements or noncompliances in a timely manner. A significant deficiency is a control deficiency, or combination of control deficiencies, that adversely affects the agency's ability to initiate, authorize, record, process, or report data reliably such that there is more than a remote likelihood that a misstatement of the Commonwealth's financial statements or a noncompliance of requirements applicable to major federal programs that is more than inconsequential will not be prevented or detected by the agency's internal control.

A material weakness is a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements or a material noncompliance of requirements applicable to major federal programs will not be prevented or detected by the agency's internal control.

105 SEA HERO ROAD, SUITE 2
FRANKFORT, KY 40601-5404
TELEPHONE 502.573.0050
FACSIMILE 502.573.0067
WWW.AUDITOR.KY.GOV

Our consideration of internal control was for the limited purpose described above and would not necessarily identify all deficiencies in internal control that might be significant deficiencies or material weaknesses. All material weaknesses and significant deficiencies over financial reporting noted during our audit, including those related to the Department of Education, if any, are reported in the Statewide Single Audit of Kentucky (SSWAK) - Volume I. All material weaknesses and significant deficiencies over compliance with requirements applicable to major federal programs, including those related to the Department of Education, if any, are reported in the SSWAK – Volume II. Control deficiencies identified in our audit for the Department of Education that were not classified as either significant deficiencies or material weaknesses are attached to this letter.

Compliance and Other Matters

As part of obtaining reasonable assurance about whether the Commonwealth's financial statements are free of material misstatement, we performed tests of the Department of Education's compliance with certain laws, regulations, contracts and grant agreements that could have a direct and material effect on the financial statements. However, providing an opinion on compliance with those provisions was not an objective of our audit, and accordingly, we do not express such an opinion. All material noncompliances related to financial reporting, as well as material instances of fraud, abuse or other matters related to financial reporting noted during our audit, including those related to the Department of Education, if any, are reported in the SSWAK – Volume I.

The Commonwealth's major federal programs are identified in the summary of auditor's results section of the SSWAK – Volume II, including any of those administered by the Department of Education. Compliance with the laws, regulations, contracts, and grants applicable to its major federal programs is the responsibility of management. Our responsibility is to express an opinion on the Commonwealth's compliance based on our audit. That opinion, as well as any material noncompliance with requirements applicable to each major program, including those related to major programs administered by the Department of Education, has also been provided in the SSWAK – Volume II.

This communication is intended solely for the information and use of management and others within the agency, and is not intended to be and should not be used by anyone other than these specified parties.

Sincerely,

Crit Luallen
Auditor of Public Accounts

FINANCIAL STATEMENT FINDINGS

Control Deficiencies Relating to Internal Controls and/or Instances of Noncompliance

FINDING 2007-KDE-IT-01: The Kentucky Department of Education Should Implement Payment Review To Ensure Appropriate Association With Contracts

During our FY 2007 audit of contracts issued by the Kentucky Department of Education (KDE) related to Software Technology, Inc. (STI), International Business Machines (IBM) Corporation, Process, Inc., (Process), and Keane, Inc. (Keane), we found that payments were made to these vendors outside the designated contract period. The Commonwealth of Kentucky purchases the Student Information System applications from STI and the MUNIS application from Process. Each Kentucky school district has their own copy of MUNIS, which must be run from IBM servers. Keane is one of six Systems Development Services vendors that are under contract with the state to provide IT system contractors.

There were six specific instances noted where a payment was issued to one of these vendors, but the payment document did not properly attribute the transaction to the appropriate contract. One instance related to a payment of $6,186.00 made to IBM for a storage expansion unit for the STI system. Two of these instances related to payments made to STI for annual licensing fees for $1,701.00 and $2,247.20, respectively. Another instance related to a payment of $1,600.00 made to Process for technical support and service for MUNIS. The final two instances relate to payments made to Keane for contract work performed within September 2006 in the amount of $8,490.00 and $3,594.00, respectively.

When payments are not properly attributed to contracts, the agency runs the risk of over-expending established limitations or paying for unauthorized services.

According to the Finance and Administration Cabinet Policy statement FAP 111-45-00 entitled Payment Documents, "An agency shall select the appropriate payment method for all goods and services…all payments referencing contracts and awards established in the state's procurement system shall be made in the state's procurement system and reference the appropriate award."

Recommendation

We recommend KDE management strengthen review over payments associated with vendors where a known contract is established to ensure that payments are attributed to the proper procurement award document.

Management's Response and Corrective Action Plan

The Kentucky Department of Education ("KDE") concurs that payments should reasonably be attributable to the proper procurement award document. It appears

FINANCIAL STATEMENT FINDINGS

Control Deficiencies Relating to Internal Controls and/or Instances of Noncompliance

FINDING 2007-KDE-IT-01: The Kentucky Department of Education Should Implement Payment Review To Ensure Appropriate Association With Contracts (Continued)

Management's Response and Corrective Action Plan (Continued)

that several of these payments were made off-contract, because of errors which occurred with the data conversion in eMARS, which made payment with the associated contract difficult. The Director for the Division of Financial and Materials Management will work with the appropriate staff in the Division of Financial and Materials Management to make them aware of this finding and emphasize the importance of associating payments with contracts.

FINDING 2007-KDE-IT-02: The Kentucky Department of Education Should Develop a Formal Disaster Recovery Plan

As noted in the prior audit of system controls at KDE, we found that for FY 2007 KDE had not developed or implemented a formalized Disaster Recovery Plan to address the backup and recovery of critical business servers, applications, and data in the case of a prolonged interruption. We are aware that KDE has designated a disaster recovery lead and has developed a policy statement related to the backup of information and data resources noted as critical; however, a comprehensive Disaster Recovery Plan has not been completed.

We noted that OET piloted a new backup system in February 2007. More than half of the systems currently requiring backup have been migrated to DPM backups. The remaining systems will be backed up with alternative mechanisms until a full migration can be completed. OET is in the process of reviewing systems within KDE to determine any that may need backup procedures, but are currently not being covered by either the new backup system or other means. There were 36 servers identified by OET that are currently not being backed up, but should be considered for the establishment of backup procedures.

We also noted OET has provided the Kentucky school districts with guidelines to assist with the backup of critical programs and data files. Further, Tyler Technologies has developed a Disaster Recovery Service for the MUNIS application. This service is available through the MUNIS contract and has currently been contracted by 16 districts, or 9.2 percent of the total 174 school districts.

Failure to develop and implement a formalized disaster recovery plan increases the possibility of loss due to excessive recovery time, costs, and disruption of processing capabilities in the case of a disaster or extended system outage.

FINANCIAL STATEMENT FINDINGS

Control Deficiencies Relating to Internal Controls and/or Instances of Noncompliance

FINDING 2007-KDE-IT-02: The Kentucky Department of Education Should Develop a Formal Disaster Recovery Plan (Continued)

Good management practices minimize risks through planning. The goal of a disaster recovery plan is to improve preparedness for extended system outages at minimal cost using available resources. Disaster Recovery Plans should be documented, approved, properly distributed, tested on a consistent basis, and updated as needed.

Recommendation

We recommend OET continue to work toward the development of a comprehensive Disaster Recovery Plan. This comprehensive plan should include an overall Disaster Recovery Plan for the Cabinet, but also a specific plan for each of the KDE offices and departments.

These individual plans should be reviewed and updated annually as necessary to reflect accurate information related to:

- Emergency personnel contacts,
- Potential alternative processing sites,
- System descriptions and process requirements,
- Backup procedures,
- Designation of on-site and off-site storage facilities,
- Backup and retention schedules for electronic media,
- Procedures to recover data from backup media, and
- Planned testing procedures.

Once completed, the comprehensive plan should be distributed to key personnel. Training on the disaster recovery procedures should be provided to these key personnel. Further, annual testing should be performed to ensure that all necessary personnel are aware of their respective roles in the implementation of the plan.

We also recommend OET continue to encourage all Kentucky school districts to develop a Disaster Recovery Plan that, at a minimum, addresses the backup and recovery of their MUNIS servers. The benefits of the Disaster Recovery Service through MUNIS should be discussed with all school districts that are currently not using this functionality. OET or another central level oversight authority should be assigned to review and approve all school district's contingency plans.

FINANCIAL STATEMENT FINDINGS

Control Deficiencies Relating to Internal Controls and/or Instances of Noncompliance

FINDING 2007-KDE-IT-02: The Kentucky Department of Education Should Develop a Formal Disaster Recovery Plan (Continued)

Recommendation (Continued)

These individual plans should be reviewed and updated annually as necessary to reflect accurate information related to:

- Emergency personnel contacts,
- Potential alternative processing sites,
- System descriptions and process requirements,
- Backup procedures,
- Designation of on-site and off-site storage facilities,
- Backup and retention schedules for electronic media,
- Procedures to recover data from backup media, and
- Planned testing procedures.

Once completed, the comprehensive plan should be distributed to key personnel. Training on the disaster recovery procedures should be provided to these key personnel. Further, annual testing should be performed to ensure that all necessary personnel are aware of their respective roles in the implementation of the plan.

We also recommend OET continue to encourage all Kentucky school districts to develop a Disaster Recovery Plan that, at a minimum, addresses the backup and recovery of their MUNIS servers. The benefits of the Disaster Recovery Service through MUNIS should be discussed with all school districts that are currently not using this functionality. OET or another central level oversight authority should be assigned to review and approve all school district's contingency plans.

Finally, we recommend OET review information and applications residing on all servers to determine whether backup procedures are warranted. For those servers that require backup procedures, but do not currently possess them, we recommend that OET develop the necessary steps to ensure that all information and data resources are properly backed up and stored.

Management's Response and Corrective Action Plan

The Kentucky Department of Education ("KDE") agrees to coordinate internally, to discuss these recommendation(s) and to determine what further actions may be appropriate, in light of these recommendations.

FINANCIAL STATEMENT FINDINGS

Control Deficiencies Relating to Internal Controls and/or Instances of Noncompliance

FINDING 2007-KDE-IT-02: The Kentucky Department of Education Should Develop a Formal Disaster Recovery Plan (Continued)

Management's Response and Corrective Action Plan (Continued)

OET is embarking on a multi-phased business continuity planning process (disaster recovery). The first phase will focus on conducting a business impact analysis to identify recovery needs and confirm our data backup needs. Any gaps between the business impact analysis/data backup needs and the current backup processes will be addressed. This phase will also develop additional processes to assure ongoing review and analysis of needs and backup strategy. This phase will be followed by a plan development phase. It is important to note that in the backup documentation provided, the systems listed as future considerations do not contain critical data. These systems could be rebuilt without backups. However, previous analysis concluded that recovery would be quicker and require less resources if done from backups. Size limitations of the current backup hardware does not allow for backups. However, in the future when additional hardware is purchased, these systems may be backed up for ease of recovery.

FINDING 2007-KDE-IT-03: The Kentucky Department of Education's Office of Education Technology Should Update And Consistently Apply Its Change Management Process

As noted during the previous audit, the program modification process developed by OET is not sufficient to ensure that only authorized changes to the IT environment, which includes the MUNIS system, are made.

Within FY 2007, OET made significant improvements to its program change control process by developing and implementing a formalized Change Management Policy and Procedures manual. This manual stipulates that changes made to the IT environment must be documented on a properly completed and approved Request for Change (RFC) form. However, the current process and RFC form does not address the identity of the person performing testing of a proposed change, migrating the change to production, or the dates when these actions were completed. This lack of information could lead to a segregation of duties issue between the request for change, development of the change, testing of the change, and promotion to production. It could also lead to a failure to complete any one of these tasks.

FINANCIAL STATEMENT FINDINGS

Control Deficiencies Relating to Internal Controls and/or Instances of Noncompliance

FINDING 2007-KDE-IT-03: The Kentucky Department of Education's Office of Education Technology Should Update And Consistently Apply Its Change Management Process
(Continued)

The Forward Schedule of Changes (FSC), which acts as a log of ongoing and completed changes to the IT environment, is not being consistently updated to show when a requested change was completed. Further, this log, along with the Change Management Calendar, is stored in an OET public folder to which OET employees have the ability to write and alter. This situation increases the risk that unauthorized or inaccurate changes could be made to the FSC log or Change Management Calendar.

Furthermore, the Change Management Advisory (CAB) meeting minutes, which are used to document discussions of current and proposed changes, are not marked to indicate who attended the weekly meeting, or who provided formal approval.

Our examination of 13 RFC forms related to changes specific to MUNIS revealed that the use of digital signatures has not been implemented within the Remedy Change Management module yet. We are aware that OET is working to implement this functionality. However, until this process is complete, there is not sufficient information maintained within the documentation to determine who provided an approval for a change. Furthermore, OET has not developed a listing of authorized Requesters/Owners who can request a change to the IT environment. These two features should be developed and used in conjunction to ensure only authorized requests are processed.

Finally, changes to the KDE utilities are not tracked through the OET change management process. However, OET does use a tracking spreadsheet. Our examination of this spreadsheet revealed that two out of five changes to a distribution utility, or 40 percent of the population, could not be traced back to the actual program code. Further a review of**)** another KDE utility showed that there were 14 changes made to the code; however, these changes are not logged within the tracking spreadsheet. In addition, the tracking spreadsheet used by OET does not identify who made the change, performed the testing, or placed the change into production.

Failure to properly apply and monitor change control procedures increases the risk that incorrect or unauthorized changes could be made to critical applications and, potentially, be moved into the live production environment.

FINANCIAL STATEMENT FINDINGS

Control Deficiencies Relating to Internal Controls and/or Instances of Noncompliance

FINDING 2007-KDE-IT-03: The Kentucky Department of Education's Office of Education Technology Should Update And Consistently Apply Its Change Management Process (Continued)

Program modification control procedures should be consistently applied in order to ensure that only appropriately authorized changes to critical applications are made and implemented within the production environment. All program modifications are to be monitored and thoroughly documented, with procedures established to log all program change requests, review and approval processes to be followed, and supporting documentation to be maintained for the process.

Recommendation

We recommend OET expand upon their formalized Change Management Policy and Procedure manual to address specific procedures required for documentation of individuals responsible for performing the changes, testing the changes, and moving changes into production. Responsible individuals should be required to sign and date the RFC form in order to avoid segregation of duties issues. This process should be attributed to changes for both the IT environment and the OET utilities.

OET should implement the use of digital signatures within its Remedy Change Management module. This feature should be used in conjunction with an authorized requester listing to ensure only authorized individuals are allowed to request and authorize changes.

OET should also ensure that CAB meeting minutes are thoroughly completed to show who was in attendance and who provides formal approval. This process will help ensure that all parties involved with a change are in agreement with what was discussed.

Furthermore, the Change Manager responsible for updating the FSC should ensure that completion dates are properly recorded for each change. Documentation such

FINANCIAL STATEMENT FINDINGS

Control Deficiencies Relating to Internal Controls and/or Instances of Noncompliance

FINDING 2007-KDE-IT-03: The Kentucky Department of Education's Office of Education Technology Should Update And Consistently Apply Its Change Management Process
(Continued)

Recommendation (Continued)

as the FSC and CM Calendar should be secured so that only authorized individuals have write or alter access to strengthen the control over unauthorized changes.

Management's Response and Corrective Action Plan

The Kentucky Department of Education ("KDE") agrees to coordinate internally, to discuss these recommendation(s) and to determine what further actions may be appropriate, in light of these recommendations.

Guidance will be documented as to the responsibility of the individuals to provide input to the Request for Change as to who is initiating the change builder functionalities, building the change, devising the back-out plan and testing plans, testing the change, and who is implementing the change.

OET is in the process of upgrading the basic Remedy module. This project is scheduled to be completed by October, 2007. Upon completion of this upgrade, it is planned to implement the Remedy Change Management Module. The Change Management Module will support the use of digital signature. We are presently authorizing anyone employed in OET to submit a Request for Change including vendors that have Service Level Agreements with the organization. We utilize the Team Leads and the Operations Managers to approve the request before being submitted to the Change Advisory Board. The team leads and operations managers validate the need or authenticity for the change before the submission. The organizational chart is used as the medium to validate employment and who are the team leads and operational managers. This is in keeping with recommended best IT business practices.

The check and balances will be enhanced in regards to the minutes to assure that the attendance is accurately validated. This will be accomplished through the Change Manager and Customer Service Center Manager who formally approves the minutes. Minutes will not be approved unless the attendance is reflected. Effective July 18, 2007 the minutes are now being approved via the Customer Service Center Operations Manager.

FINANCIAL STATEMENT FINDINGS

Control Deficiencies Relating to Internal Controls and/or Instances of Noncompliance

FINDING 2007-KDE-IT-03: The Kentucky Department of Education's Office of Education Technology Should Update And Consistently Apply Its Change Management Process (Continued)

Management's Response and Corrective Action Plan (Continued)

FSC (Forward Schedule of Changes) is a document that contains details of all the Changes approved for the implementation and their proposed implementation dates. The RFC is the formal documentation that is used to track the dates, closures/completions and other data, not the FSC. The FSC is an aid in tracking proposed scheduled changes. We have added the columns Actual Completed in the completed tab per this finding; however, this is not a recommended best practice and is redundant data since the work is captured in the RFC. OET will assess if there is any added benefits and if not, the columns will be removed.

FINDING 2007-KDE-IT-04: The Kentucky Department of Education's Office of Education Technology Should Ensure That No Shared Accounts Are Present on Agency Machines

Our FY 2007 audit of KDE system controls revealed OET had not adequately secured system access to the OET gateway server and FTP server, which are utilized in the transmission of MUNIS data.

Specifically, two generic user IDs were established with access to the FTP server that were being shared by two users. Five generic user IDs were established with access to the gateway server that were being shared by anywhere from 2 to 11 different users. The one account that was being shared by 11 different users was an application account utilized to access MUNIS at the district level. In this case the access level granted was Read-Only access to MUNIS data. This same-shared account was noted in the previous audit, but with greater than Read Only access. This is an improvement, but the issue of a shared generic account is still an issue. We had also noted OET's lack of procedures for monitoring security logs, but that issue was addressed in a separate comment.

We further noted that one account established with access to the FTP server for Jefferson County use was not assigned to a specific user and OET was unsure of the individual(s) using that account. Due to the size of their reports, Jefferson County was provided direct access to the FTP server to upload their district's MUNIS reports.

FINANCIAL STATEMENT FINDINGS

Control Deficiencies Relating to Internal Controls and/or Instances of Noncompliance

FINDING 2007-KDE-IT-04: The Kentucky Department of Education's Office of Education Technology Should Ensure That No Shared Accounts Are Present on Agency Machines (Continued)

Weaknesses in logical security controls may increase the opportunity for unauthorized modification to files and computers, as well as misuse of computer resources. The use of shared system accounts does not allow for an adequate audit trail of system activity. Further, failure to assign primary users to system accounts does not provide an adequate audit trail and increases the risk of unauthorized or inappropriate transaction submissions.

System access should be limited to the level necessary for performing assigned duties. Furthermore, it is not good practice to employ shared system accounts. On the contrary, each user should have an individually assigned account so that their activity can be properly identified and logged. In addition, OET should ensure only authorized users are assigned to all system access accounts, including the Jefferson County account.

Recommendation

We recommend OET discontinue the practice of employing shared user accounts on its servers. Instead, all authorized KDE users should be assigned individual accounts so that their activity can be properly identified and logged on the OET servers. In addition, OET should identify the user of the Jefferson County School District account in order to ensure that the user is authorized to transfer MUNIS data to the OET server. OET should periodically review all user accounts with access to their servers in order to ensure the continued propriety and necessity of the account.

Management's Response and Corrective Action Plan

The Kentucky Department of Education ("KDE") agrees to coordinate internally to discuss these recommendation(s) and to determine what further actions may be appropriate, in light of these recommendations.

FINANCIAL STATEMENT FINDINGS

Control Deficiencies Relating to Internal Controls and/or Instances of Noncompliance

FINDING 2007-KDE-IT-05: The Kentucky Department of Education Should Ensure That All Open Ports On Agency Machines Have A Business-Related Purpose

While performing the security vulnerability assessments for FY 2007 for machines controlled by KDE, our examination identified 3 out of 305 machines, or 1.0 percent of the population, were found to have port 21, FTP, open during FY 2007. The agency has been reviewing the necessity of the FTP service on these machines and has closed the service on the first machine, decommissioned the second machine, and is in the process of investigating the need for the service on the third machine.

For security purposes, detailed information that would identify the specific servers or user accounts that contributed to these findings is being intentionally omitted from this comment. However, these issues were thoroughly documented and communicated to appropriate agency personnel.

The existence of unused or unnecessary open ports increases potential security vulnerabilities and is an invitation for intruders to enter the system.

To minimize the risk of unauthorized access to a machine, only necessary, business-related ports should be open.

Recommendation

We recommend KDE complete the review of the machines with port 21 open to ensure there is a specific business-related purpose requiring the port to be open. If not required, then that port should be closed. If the port is necessary, then KDE should ensure the software has a current license, the most recent patches are implemented for the service in use, and adequate logical security controls are implemented to prevent unauthorized access as necessary.

Management's Response and Corrective Action Plan

Three machines were found to have port 21 open during FY 2007. The agency has reviewed the necessity of the FTP service on these machines and has decommissioned the second and third machines and has determined that first is necessary for business-related purposes. The OS on the remaining machine was licensed with the purchase of the hardware and the patches are up-to-date; however, there are not currently any patches being released for the version of the software being used. This system houses financial reports that are automatically generated on district's financial servers and transferred to this server via Secure Shell (SSH).

FINANCIAL STATEMENT FINDINGS

Control Deficiencies Relating to Internal Controls and/or Instances of Noncompliance

FINDING 2007-KDE-IT-06: The Kentucky Department of Education Should Ensure That All Agency Web Servers Have Updated Software and Security Patches Installed

During the security vulnerability assessments for FY 2007, our examination revealed web service vulnerabilities with three machines controlled by KDE. The majority of the web service vulnerabilities appear to result from outdated or unpatched software. These vulnerabilities can potentially be exploited, leading to exposure of sensitive system information or misuse of the services the web server provides.

For security purposes, detailed information concerning the specific machines or user accounts that contributed to these findings is being intentionally omitted from this comment. However, these issues were thoroughly documented and communicated to the appropriate agency personnel.

If machines within a network have web services running that allow the above security issues, the stability of the network could be compromised as these machines become more susceptible to unauthorized intrusion. Installed web services without a specific business purpose may subject the network to buffer overflow issues, execution of arbitrary commands to circumvent network security, and unnecessary access to view network server volume files.

To assist in securing a network adequately, it is necessary to ensure all required web services have the most current security patch installed or disable any web service that does not have a known business function.

Recommendation

We recommend KDE take the necessary actions to ensure that web services on each identified machine are appropriately updated or patched.

Management's Response and Corrective Action Plan

OET has reviewed all web services identified and is comfortable that all such services are appropriately configured for normal operations.